IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

PROGRAMME
OCÉAN ET
FONDS MARINS

QUEL PARTENARIAT POUR LA MARINE NATIONALE AVEC LES ACTEURS DE L'ÉCONOMIE MARITIME ?

Tancrède Wattelle / Doctorant, École navale/CNAM

Avril 2026

PRÉSENTATION DE L'AUTEUR

Tancrède Wattelle / Doctorant, École navale/CNAM

Tancrède Wattelle est en deuxième année de doctorat en sociologie de l'innovation en cotutelle CNAM et École navale. Ses recherches portent sur les enjeux doctrinaux, organisationnels et sociotechniques de l'application de la supériorité informationnelle au combat naval.

PROGRAMME
OCÉAN ET
FONDS MARINS

Dirigé par Julia Tasse, le programme Océan et fonds marins de l'IRIS est un programme de recherche transdisciplinaire, qui étudie la géopolitique de la mer, la gouvernance de l'océan et des fonds marins ainsi que les implications sécuritaires des transitions climatiques, énergétiques et numériques dans le maritime..

Ce programme porte le projet de recherche pluriannuel Ocean Stewardship. Il est partenaire de projets de recherche financés par l'Agence nationale de la recherche (PEPR BRIDGES et GetMoreH2).

Le programme travaille avec des universités partenaires et des acteurs institutionnels comme l'Agence française de développement, la Marine nationale ou encore l'Agence nationale de la recherche.

---

iris-france.org

@InstitutIRIS
@InstitutIRIS
institut_iris
IRIS
IRIS - Institut de relations internationales et stratégiques

À partir de la fin de 2023, la recrudescence des attaques houthies en mer Rouge contre des navires marchands a profondément perturbé les flux commerciaux dans la zone. Entre décembre 2023 et janvier 2024, entre 70 % et 80 % des navires de commerce ont ainsi été déroutés pour éviter le détroit de Bab el-Mandeb[1]. Tandis que certains armateurs ont privilégié le détour par le cap de Bonne-Espérance, d'autres préfèrent modifier leur comportement habituel en se rapprochant des côtes africaines, en communiquant avec la rébellion[2] ou en misant sur la discrétion. Cette diversité des réactions n'a pas empêché l'attaque de plusieurs vecteurs par missile ou drone.

Le caractère inédit de la crise par l'aspect protéiforme de la menace (modes opératoires innovants, dimension informationnelle, résonance locale d'une crise régionale) a pris de court les armateurs, les institutions internationales ainsi que plusieurs marines. Le déploiement subséquent de bâtiments de combat en mer Rouge doit assurer la protection du trafic commercial, notamment sous forme d'escortes de convois. Les difficultés constatées dans l'interaction avec les acteurs de l'économie maritime ont entraîné un rappel à l'ordre de la part des principales associations d'armateurs[3]. Alors que les intérêts maritimes retrouvent leur rôle de cible à part dans la conflictualité sous le seuil entre puissances, l'efficacité du partenariat entre une marine et les acteurs de l'économie maritime redevient un enjeu majeur, à plus forte raison quand ils partagent le même pavillon.

La France a reconnu dans le Livre Blanc de 2013[4] l'interdépendance entre le dynamisme de l'économie nationale, désormais qualifiée d'espace de souveraineté, et la vitalité du commerce international, assuré en majorité par le transport maritime. Depuis treize ans, son patrimoine maritime a de surcroît augmenté à la faveur de l'émergence de l'éolien *offshore*, de la densification des câbles sous-marins et de la montée en puissance de l'armateur CMA-CGM. Dans cette continuité, la *Revue nationale stratégique* (RNS) de 2025 perpétue la volonté française de pérenniser ses accès dans les espaces communs, notamment l'aéromaritime et les fonds marins, tout en contrant les « acteurs hostiles ». En particulier, la fonction stratégique de connaissance et d'anticipation est mise en avant pour dissiper une incertitude toujours aussi prégnante dans le milieu maritime[5] et ainsi surmonter « l'inconfort opératif »

[1] Notteboom, T., Haralambides, H., & Cullinane, K., « The Red Sea crisis: Ramifications for vessel operations, shipping networks, and maritime supply chains », *Maritime Economics & Logistics* (2024).
[2] Loh, M., « Some ships in the Red Sea have declared themselves "all Chinese," seemingly in hopes of avoiding Houthi attacks », *Business Insider* (15 janvier 2024).
[3] Scheffer, H., « Mer Rouge : nouvelles consignes de sécurité pour les armateurs », *Le Marin*, *Ouest France* (6 février 2024).
[4] République française, « Livre blanc sur la défense et la sécurité nationale 2013 », *La Documentation française* (2013).
[5] Lavernhe Thibault, Corman François-Olivier, *Vaincre en mer au XXIe siècle*, Les Équateurs, 2023.

évoqué par l'amiral Vandier[6] pour désigner la prolifération des manœuvres, notamment asymétriques, sous le seuil de conflictualité.

En sus de la protection de son économie maritime, la puissance navale française doit donc esquisser un grand écart entre combat conventionnel de haute intensité et anticipation de modes opératoires hybrides. Pour y parvenir, elle peut exploiter pleinement la valeur ajoutée des mêmes acteurs économiques qu'elle doit défendre dans le cadre d'un partenariat équilibré. En particulier, la capacité à recueillir, traiter et diffuser de l'information peut concourir à améliorer l'appréciation de situation du milieu maritime (ou *Maritime Domain Awareness*, MDA[7]) et optimiser la prise de décision de chacun dans la temporalité des opérations.

EXPLOITER DAVANTAGE LES SYNERGIES

Un partenariat avant tout institutionnel

En France, la collaboration entre les services de l'État (Marine nationale, gendarmerie maritime, douanes, affaires maritimes) et les acteurs de l'économie maritime reste marquée par les obligations administratives mutuelles, incluant la préparation d'une éventuelle réquisition, la protection des activités et infrastructures critiques ainsi que la sécurité en mer. La loi prévoit ainsi dans l'article L2213 du Code de la défense la réquisition de moyens civils dans le cas de catastrophes naturelles ou de crises. Entérinée par la loi sur l'économie bleue de 2016, la création du concept de « flotte à caractère stratégique » est suivie en 2017 par un rapport du Conseil supérieur de la marine marchande, destiné à favoriser sa définition par décret la même année. Publié le 17 juillet 2023, le rapport du député Yannick Chenevard sur ce dispositif[8] rappelle l'absence d'avancées tangibles et propose des axes d'effort. En réponse, le gouvernement promulgue le décret du 5 juillet 2024, entérinant une concrétisation accrue du dispositif, en plus d'un contrôle naval contraignant. En particulier, le texte prévoit la préparation de cadres de mise à disposition, d'initiatives de développement de la flotte et d'un suivi annuel.

Au-delà du dispositif de réquisition, les acteurs privés échangent régulièrement avec la communauté du renseignement dans le cadre des responsabilités de protection

[6] Compte-rendu de l'audition de l'amiral Pierre Vandier sur le projet de LPM 2024 à 2030, Assemblée nationale (12 avril 2023).
[7] Bachelier, J., & Boulanger, P. « La "fusion de l'information" : levier de la puissance maritime française », IFRI (2023).
[8] Chenevard Yannick, « Rapport sur la redéfinition du dispositif de flotte stratégique », *Mission gouvernementale* (17 juillet 2023).

interministérielles. La diffusion de renseignement à des entreprises privées françaises est régie par la réglementation sur les opérateurs d'importance vitale (OIV) de 2006, qui identifie notamment depuis 2016 et 2017 les secteurs et sous-secteurs d'activité d'importance vitale (SAIV) que sont le transport maritime, l'alimentation, l'approvisionnement en énergie ou encore les communications électroniques et Internet. À ce titre, un plan de protection des entreprises critiques est établi, des responsables de l'économie maritime habilités et leurs systèmes d'information régulièrement audités afin de recevoir des données sensibles. En particulier, l'augmentation des actions de lutte informatique offensive contre les entreprises, perpétrées par des groupes liés à des compétiteurs, a contribué à développer la coopération.

Au niveau opérationnel, une convention sur le contrôle naval volontaire (CNV) associe dès juin 2001 la Marine avec 18 armateurs signataires[9]. Elle comprend la signalisation des mouvements des navires civils afin de mieux appréhender les transits du pavillon français ainsi que la transmission d'informations par la Marine nationale concernant la sécurité des zones traversées par ces mêmes vecteurs. Alors que le partage d'information se développe à l'international avec la création en 2007 du centre opérationnel d'analyse du renseignement maritime pour les stupéfiants (MAOC-N) de Lisbonne, de l'Information Fusion Cell (IFC) de Singapour en 2009 ou encore du Maritime Information Cooperation & Awareness Center (MICA Center) de Brest en 2016, la CNV évolue en 2019 pour devenir la coopération navale volontaire, incluant la remontée d'informations d'intérêt ou encore le partage de retour d'expérience. La coopération est aussi concrète. La prise d'otages du voilier *Ponant* en 2008 motive ainsi la mise en place de l'embarquement d'équipes de protection embarquées (EPE) de la Marine à bord de vecteurs civils français évoluant dans les zones à risque. Néanmoins, elles sont progressivement remplacées à partir de 2015 par des opérateurs privés fraîchement agrémentés. Si des EPE embarquent encore sur des navires civils, leurs déploiements restent sporadiques comparativement à la crise de la piraterie somalienne.

Si le cadre du partenariat public-privé a été clarifié, il ne constitue pas pour autant un dispositif efficace permettant l'optimisation de la valeur ajoutée de chacun, tout particulièrement dans la temporalité des opérations.

Des opportunités prometteuses

Le développement tous azimuts de l'économie maritime française s'est décliné par l'émergence de compétences à forte valeur ajoutée, doublée d'une capacité de captation et de traitement complémentaire de l'information disponible en source ouverte.

[9] Guy Guernon (de), « Le contrôle naval volontaire », *Revue Défense nationale*, n° 656, p. 81-84 (août-septembre 2003).

Si ce constat est particulièrement adapté aux zones littorales françaises où l'activité est la plus dense (pêche côtière, éolien *offshore*, transport de passagers), le pavillon français transite également à l'international grâce aux armateurs du transport maritime et de croisière, voire dans le cadre d'activités moins connues comme la pose de câbles sous-marins, la prospection et l'exploration. La montée en puissance du groupe tricolore CMA-CGM permet ainsi de disposer de capteurs d'opportunité[10] sur tous les océans du globe grâce à sa flotte d'environ 680 navires de commerce à capacité hauturière. En outre, plusieurs acteurs privés mettent en œuvre des capacités spécialisées de recueil, notamment dans l'espace sous-marin et des grands fonds par le biais des navires câbliers. Certains opérateurs recueillent également la production en temps réel des senseurs des câbles[11] destinés à protéger les infrastructures sous-marines critiques. Enfin, ces opérateurs disposent d'accès inédits pour les services de l'État. Un pays mis au ban des nations pourra ainsi difficilement être visité par une unité représentant l'État français sans répercussions médiatiques et diplomatiques. À l'inverse, un navire de commerce dûment orienté au préalable pourra facilement prendre le pouls de la situation locale. Ce constat vaut tout particulièrement pour les exploitants de concessions portuaires et de terminaux à conteneurs. Enfin, l'émergence d'entreprises nationales en charge de la protection de navires comme Prorisk permet de disposer de l'expertise d'agents familiers des attentes de la Marine nationale. Ce type de mode opératoire semble déjà pratiqué par la Russie, comme en témoigne l'arraisonnement du *Boracay*[12].

La perception privée du milieu aéromaritime est complétée par de la donnée privée et disponible en libre accès. De l'imagerie satellitaire commerciale et en source ouverte aux flux des *webcams* littorales en passant par les transpondeurs de navires *Automatic Identification System* (AIS) et d'aéronef *Automatic Dependent Surveillance Broadcast* (ADSB), les capteurs se sont multipliés. De plus, leur couverture a drastiquement augmenté à l'aune de la révolution satellitaire du *New Space* et de l'avènement des réseaux sociaux. Désormais, une donnée autrefois diffusée localement comme l'AIS peut faire l'objet d'une exploitation exhaustive au niveau planétaire dans des délais très courts[13]. Pour sa part, l'imagerie du programme européen *Copernicus* n'a jamais été aussi précise, disponible aussi rapidement et dans des conditions d'accessibilité aussi avancées[14]. De la donnée brute peut également être

[10] Système ou plateforme dont la fonction première n'est pas le recueil de renseignements.

[11] Eleftherakis, D., & Vicen-Bueno, R., « Sensors to Increase the Security of Underwater Communication Cables: A Review of Underwater Monitoring Sensors », *Sensors,* 20, 737 (2020).

[12] « Espionnage : des agents de sécurité russes à bord de la flotte fantôme près des côtes européennes », *France 24* (23 février 2026).

[13] Yang, Y., Liu, Y., Li, G., et al., « Harnessing the power of Machine learning for AIS Data-Driven Maritime Research », *Transportation Research Part E: Logistics and Transportation Review,* 183 (2024).

[14] Ray William, Zlinszky Andras, « Accessing Sentinel mission data via the new Copernicus Data Space Ecosystem APIs », *Copernicus* (28 septembre 2023).

recueillie directement grâce aux réseaux sociaux, permettant de relocaliser des navires civils ou militaires dans les ports ou les *choke-points*. En avril 2020, le *think tank* C4ADS a ainsi publié une enquête fournie sur les livraisons maritimes de gaz naturel liquéfié iranien à la Chine[15]. Pour cela, le centre d'études a croisé les sources de données que sont l'AIS, l'imagerie satellitaire commerciale ou encore les registres maritimes. Par la suite, cette manœuvre de renseignement en source ouverte a également été employée afin de mettre en évidence le recours au transport par la mer Caspienne pour les livraisons de drones iraniens vers la Russie[16]. Ces exemples illustrent la pertinence du renseignement en source ouverte et de la méthodologie multicapteurs dans la compréhension de l'hybridation croissante sur et sous les mers.

Tant pour les acteurs de l'économie maritime que pour les services de l'État, l'exploitation de ces flux reste une obligation pour compléter son MDA ainsi qu'un défi.

SURMONTER LES DÉFIS DE L'INFORMATION MARITIME

Un champ informationnel global incertain

Par sa faculté à co-localiser, recouper et analyser des flux multisources différents (transpondeurs, satellitaire, réseaux sociaux), le champ informationnel global dédié à l'espace aéromaritime représente autant une opportunité qu'un défi par l'incertitude qu'il génère, suscitant l'intérêt des puissances, mais aussi d'entités criminelles (trafiquants, pirates, pêche illégale).

Avant tout, chaque type d'acteur cherche à préserver la sécurité de ses opérations en se prémunissant d'une détection d'opportunité. Pour plusieurs groupes criminels, cela consiste avant tout à employer des embarcations modestes et discrètes (*dhows*, *skiffs*, boutres), voire des submersibles improvisés pour certains trafiquants de drogue. Si la majorité des entités étatiques ou encore les pêcheurs illégaux ne se reporteront tout simplement pas, le camouflage permet de limiter l'information diffusée. Un rapport du département de la défense américain sur la mer de Chine du Sud met ainsi en évidence les efforts des forces chinoises de la zone pour camoufler leurs unités et leurs installations, allant jusqu'à installer

[15] « A Hull in Their Story: Satellite imagery, AIS, and the Ships Secretly Transporting Iranian Gas to China », *C4ADS* (23 avril 2020).
[16] Nelson Haley, « Dark Deals on the Caspian: How Iran Ships Drones to Russia », *Caspian Policy Center* (21 août 2023).

des leurres[17]. Même les flux vidéo littoraux font désormais l'objet d'une vigilance accrue de la part des marines. L'*US Navy* a ainsi demandé la désactivation de plusieurs *webcams* couvrant les approches de la base de San Diego en 2023[18].

L'intégrité des flux informationnels globaux peut également être remise en question afin de proposer une représentation altérée de la réalité maritime. La falsification représente le premier niveau de complexité, allant de reports imprécis par facilité à de véritables usurpations intentionnelles d'identité. Le caractère déclaratif des systèmes AIS et ADSB concoure directement à ce phénomène, tandis que le format satellitaire reste encore peu adapté à la falsifiabilité[19]. La simulation de données représente le niveau suivant, incarné par une manœuvre cyber complexe. Des reports AIS localisant le destroyer russe *Marshal Ustinov* en mer de Norvège ont ainsi été mis en évidence à plusieurs reprises, malgré son absence de la zone[20]. Dans un dernier temps, la donnée brute peut être diffusée de manière plus ou moins démarquée sur les réseaux sociaux dans le cadre d'une manœuvre informationnelle élaborée. En fonction de l'attribuabilité envisagée, c'est un compte officiel ou un réseau d'avatars qui tenteront de cibler une audience prédéterminée et si possible de diluer par la viralité un narratif appuyé sur un contenu plus ou moins altéré.

Dans un environnement informationnel global investi tant par les puissances que par les groupes criminels, une démarche mutualisée peut ainsi enrichir de manière éclairée une MDA partagée.

Des champs immatériels locaux contestés

L'incertitude du champ informationnel *global* se double d'un investissement des champs immatériels *locaux* par une menace marquée par l'hybridité et l'incertitude.

Les champs immatériels perceptibles uniquement localement, incarnés en mer par l'électromagnétique (ondes radar, radio, satellitaire, plus rarement téléphonie mobile et Wi-Fi) et par l'acoustique sont ainsi le théâtre d'une confrontation accrue. Historiquement, le combat naval est ainsi marqué par une omniprésence de la ruse, pouvant parfois aller jusqu'à la perfidie. À l'instar du croiseur léger allemand *Emden* durant la Première Guerre mondiale, l'usurpation de pavillon ou le camouflage en navire marchand participent d'une tentative

[17] Dahm, J. M., « A survey of technologies and capabilities on China's military outposts in the South China Sea: Hardened infrastructure, counter-reconnaissance, and battlespace environment management », *U.S. Department of Defense*, *Defense Technical Information Center* (Octobre 2020).
[18] Ziezulewicz, G., « Popular San Diego web cameras removed at Navy's request », *Navy Times* (19 avril 2023).
[19] Delaunay, A., « Deepfakes géographiques : l'intelligence artificielle menace-t-elle la crédibilité de l'imagerie satellite ? », *Le Monde* (13 octobre 2021).
[20] Sutton, H. I. « Fake position reported for Russian Navy cruiser Ustinov », *Covert Shores* (2023).

d'influence sur les perceptions destinée à favoriser la discrétion, voire le rapprochement en vue d'un engagement. Avec l'invention du radar et du sonar, ces manœuvres fondées sur la seule capacité de détection visuelle se sont diversifiées avec l'émergence de simulations d'ondes radar et acoustiques. De nombreux bâtiments de combat disposent ainsi de contre-mesures électroniques (ECM), capables d'émettre une signature radar différente de la sienne, y compris celle d'un navire civil. De même, le développement de technologies et de modes opératoires se poursuit, comme l'illustre le concept de drones sous-marins agissant comme des leurres acoustiques[21].

Les acteurs non étatiques ne sont pas en reste dans ce domaine, comme l'ont démontré les Houthis en mer Rouge par leurs manœuvres informationnelles complexes. Au-delà du détournement de l'usage du système de transpondeurs[22], ils bénéficieraient par ailleurs de renseignement satellitaire partenaire[23], contribuant à améliorer la précision de leur ciblage. Leurs manœuvres d'influence se sont diversifiées et emploient désormais non seulement la radio[24], mais aussi les messageries électroniques[25]. Du brouillage GPS a même été observé, sans que sa cause ne puisse être formellement identifiée[26].

Le caractère démarqué d'une manœuvre informationnelle permet son emploi sous le seuil de conflictualité entre États, entérinant l'avènement de modes opératoires multidomaines. Une offensive cyber contre un système de report ou le remplacement d'un flux *webcam* par un autre représentent autant de modes d'action envisageables. La simulation à grande échelle de reports AIS peut ainsi permettre de brouiller le suivi dans une zone donnée, permettant à un vecteur d'y transiter en toute quiétude[27].

D'abord apanage exclusif des marines de combat, les capacités d'action dans les champs immatériels prolifèrent et se diversifient à l'aune des mutations que connaissent ces espaces. La menace gagne donc en complexité grâce à un mélange de tactiques ancestrales, de détournements d'usage et d'innovations, qui concourent à entretenir l'opacité et à accélérer la contraction du temps des opérations.

---

[21] Yoga, P. R. A., & Bautista, L., « The law of perfidy and ruses of war at sea », *Journal of Conflict & Security Law*, 29(3), pp. 375–390 (2024).
[22] Matthews Sean, « How the Houthis mined commercial intelligence to sabotage global trade », *Middle East Eye* (5 février 2024).
[23] Faucon Benoit, Grove, Thomas, « Russia provided targeting data for Houthi assault on global shipping », *Wall Street Journal* (24 octobre 2024).
[24] Evans Mary Ann, « Houthi failures lead to VHF harassment », *Container News* (3 juillet 2024).
[25] Maltezou Renee, Saul Jonathan, « Houthis' email alert to Red Sea ships: Prepare for attack, with best regards », *Reuters* (3 octobre 2024).
[26] Cogné, G., « En mer Rouge, des navires de commerce confrontés au brouillage GPS », *Mer et Marine* (16 mai 2025).
[27] Androjna, A., Perkovič, M., Pavic, I., & Mišković, J., « AIS data vulnerability indicated by a spoofing case-study », *Applied Sciences*, 11(11), 5015 (2021).

MUTUALISER LES MOYENS POUR NUANCER L'INCERTITUDE

Recueillir et authentifier la donnée

La mutualisation des moyens et des accès peut accroître l'appréciation de chacun afin de pouvoir appuyer la prise de décision dans la temporalité des opérations.

Tout d'abord, la connaissance des transits futurs et le suivi en temps réel de l'ensemble des navires civils sous pavillon français peuvent faciliter une orientation préalable. Ensuite, la mise en place d'un dispositif clair de remontées d'information à intérêt immédiat doit permettre de disposer d'une capacité de renseignement d'alerte élargie. Un lien de ce type semble déjà unir des flottilles de pêche chinoises présentes sur la majorité des océans et leurs interlocuteurs étatiques[28]. Ensuite, l'embarquement de capteurs connectés ou de personnel spécialisé sur des navires marchands peut optimiser le recueil à partir de ces vecteurs. L'installation d'un système électro-optronique de type Paseo XLR, couplé à un outil d'identification par intelligence artificielle, permettrait d'automatiser la détection visuelle.

Dans cette continuité recueil-authentification-exploitation des données, il paraît indispensable d'adapter l'ensemble des vecteurs aux défis des champs immatériels locaux. Un détecteur de *deepfake* permettra ainsi de détecter une usurpation d'identité vocale, tandis qu'une signature radio ou radar pourra faire l'objet d'une analyse technique révélant d'éventuelles altérations[29]. Pour sa part, l'installation de pare-feu adaptés peut entraver une offensive saturante par déni de service AIS. Par opportunité, les éléments embarqués pourront participer de la protection du navire en cas d'attaque. Quitte à être ciblé en raison de son pavillon, autant pouvoir contre-détecter et se défendre.

La mise en place d'un centre opérationnel de l'information maritime, actif en permanence, permettrait d'agréger et d'échanger l'information sensible entre acteurs de l'État en mer et de l'économie maritime, donnant naissance à une capacité centralisée de partage de renseignement d'intérêt maritime. En particulier, il pourrait constituer l'interface privilégiée d'échange sur la menace protéiforme en mer et les moyens de s'en prémunir. En se dotant d'une capacité d'intégration du champ informationnel global, il pourrait également y conduire une action de recueil, d'authentification et d'exploitation. Ce dispositif pourrait ainsi disposer

[28] Luo Shuxian, Panter Jonathan, « China's Maritime Militia and Fishing Fleets: A Primer for Operational Staffs and Tactical Leaders », *Military Review* (janvier-février 2021).
[29] Ray, C., Iphar, C., & Napoli, A., « Methodology for Real-Time Detection of AIS Falsification », *Maritime Knowledge Discovery and Anomaly Detection Workshop*, pp. 74-77 (2016).

d'outils spécialisés en détection de comportements suspects (disparitions, transbordements, route erratique) et de contenus falsifiés ainsi qu'en analyse de discours. En s'appuyant sur les remontées des navires en mer, il peut même comparer avec sa perception globale afin de discerner d'éventuelles anomalies.

Les écueils de la temporalité et de la véracité de la donnée peuvent donc être surmontés grâce à un lien permanent et direct entre les capteurs d'opportunité de l'économie maritime et un échelon d'exploitation en second rideau, également en charge de l'intégration du champ informationnel global.

Représenter l'information à fin d'action

La donnée authentifiée et exploitée peut alimenter un système centralisé et mutualisé de représentation destiné à accompagner la prise de décision dans la temporalité des opérations. Dans la continuité d'un rapport sur le sujet[30], l'appréhension du MDA pourrait être optimisée par la centralisation des flux en source ouverte, publics (perceptions tactiques) et privés (CNV) ainsi que l'élaboration subséquente et la mise à jour en temps réel d'une situation maritime de référence (SMR) mise à disposition de tous les opérateurs agréés (OIV) sous l'autorité du centre opérationnel de l'information maritime.

Pour cela, l'agrégation de flux multicapteurs authentifiés au sein d'un système d'information géographique (SIG) alimenté de manière automatisée et en temps réel peut proposer une visualisation exhaustive et cohérente grâce à l'optimisation de l'interprétation des données issues d'environnements complexes[31]. La variété de l'information doit être surmontée par le dénominateur commun de géolocalisation de la donnée et être représentée à l'aide d'un support cartographique. Développé par la Marine, l'outil ANAIS[32] s'inscrit dans cette continuité en agrégeant les données AIS et ADSB, les zones militaires ainsi que d'exercice. Par le géoréférencement de la donnée, le SIG peut également renforcer son degré de fiabilité ou détecter au contraire une anomalie. Grâce à l'indexation de l'espace aéromaritime qu'il propose, il peut enfin incarner une politique de gouvernance de la donnée adaptée. En s'appuyant sur ces bulles informationnelles géographiques, le SIG encourage ainsi la frugalité des flux tout en les limitant au besoin. Pour autant, la verticalité et la centralisation qui font sa force peuvent néanmoins l'empêcher de s'inscrire dans la temporalité de la menace. Pour

[30] Bachelier, V. J., & Boulanger, P., « La "fusion de l'information" : levier de la puissance maritime française », IFRI (2018).
[31] Redhu, S., & Hegde, R. M., « Multi-Sensor Data Fusion for Cluster-based Data Aggregation in IoT Applications », *2019 IEEE International Conference on Advanced Networks and Telecommunications Systems*, pp. 1-6 (2019).
[32] L'outil ANAIS (Analyse des Incohérences de Situation maritime) est une plateforme de surveillance qui agrège la donnée maritime multisource afin de détecter les anomalies et les comportements suspects en mer.

pallier cet écueil, un partage automatisé de la donnée brute entre capteurs co-localisés doit inaugurer une connexion en temps réel sur la base d'une proximité géographique temporaire.

Dans un second temps, l'amélioration de l'autonomie d'appréciation peut permettre d'accompagner la prise de décision. Fondée sur les zones d'évolution habituelles ainsi que les performances des capteurs et de l'armement, la représentation géographique de la menace permet ainsi de générer des transits alternatifs à l'écart des zones de risque. Un méthanier français franchissant le détroit de Bab el-Mandeb pourra ainsi se voir dérouter grâce à la visualisation des portées de détection, des moyens de ciblage ainsi que des portées de l'armement mis en œuvre par les Houthis. En cas de détection précoce, un processus itératif peut améliorer la prise en compte de l'aléa par des équipages peu habitués. Une fois caractérisé et identifié par les capteurs embarqués, le mode opératoire suspect peut être décliné en paramètres d'engagement (portée, guidage, charge explosive) afin de recommander une conduite à tenir à l'équipage (déroutement, confinement, abandon du navire).

À terme, la mise en place de modèles adaptés d'aide à la décision tirant parti non seulement des données de fonctionnement du navire (localisation, performances), mais aussi de l'environnement (géographie, météorologie) et de la menace peut permettre de faire face au dynamisme du temps réel. La délimitation d'une zone de dérive de mines sous l'impulsion des courants locaux représente ainsi l'une des modélisations envisageables.

L'automatisation du traitement de l'information multisource et sa représentation par un SIG centralisé, complétés par des échanges horizontaux et localisés de données, paraissent donc adaptés à une collaboration dans le temps des opérations. L'agrégation de flux de données aéromaritimes peut ensuite participer de l'amélioration du traitement des variables locales en vue d'une prise de décision ultérieure.

Dans un pays soupçonneux des relations entre services de l'État et entreprises, un rapprochement fondé sur l'obligation régalienne de protection d'une souveraineté aéromaritime contestée constitue un risque politique. Pour autant, il est illusoire d'envisager pouvoir assurer le contrôle du vaste espace aéromaritime français sans le concours actif des acteurs de l'économie maritime, légalement encadrés par le statut d'OIV au sein d'une flotte stratégique aux attributions revisitées. Sa contribution résiderait non seulement dans un recueil qualitatif et quantitatif, mais aussi dans une participation à l'exploitation automatisée, éclairée et exhaustive d'une donnée volumineuse, polymorphe et éphémère. La consolidation de l'information au sein d'un SIG agrégateur de flux et distributeur de renseignement doit permettre d'alimenter des services d'analyse et d'aide à la décision temporellement

pertinents, dont le rôle pourrait être décisif en cas de crise majeure. À terme, la participation de nos alliés dans un cadre bilatéral ou communautaire permettrait de compter sur le soutien de ce pilier de la puissance navale qu'est le partenariat[33] afin de compléter une supériorité opérationnelle placée grâce à la donnée au cœur de la suprématie navale de l'avenir.

[33] Compte-rendu de l'audition de l'amiral Nicolas Vaujour (CEMM) sur le projet de loi de finances 2024, Assemblée nationale (5 octobre 2023).

L'expertise stratégique en toute indépendance

PROGRAMME
OCÉAN ET
FONDS MARINS

IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

2 bis, rue Mercœur - 75011 PARIS / France
+ 33 (0) 1 53 27 60 60
contact@iris-france.org

iris-france.org

L'IRIS, association reconnue d'utilité publique, est l'un des principaux think tanks français spécialisés sur les questions géopolitiques et stratégiques. Il est le seul à présenter la singularité de regrouper un centre de recherche et un lieu d'enseignement délivrant des diplômes, via son école IRIS Sup', ce modèle contribuant à son attractivité nationale et internationale.

L'IRIS est organisé autour de quatre pôles d'activité : la recherche, la publication, la formation et l'organisation d'évènements.